INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

# *On dertermining mixing parameter of CC-CMA algorithm by solving semi-algebraic sets*

Nong Gu — Daniel Lazard — Fabrice Rouillier — Yong Xiang

**N° 5830**

February 2006

Thème SYM

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--5830--FR+ENG

# On dertermining mixing parameter of CC-CMA algorithm by solving semi-algebraic sets

Nong Gu [*] [†] , Daniel Lazard [‡] [§] , Fabrice Rouillier [¶] [§] , Yong Xiang [‖] [†]

Thème SYM — Systèmes symboliques
Projets SALSA

Rapport de recherche n° 5830 — February 2006 — 27 pages

**Abstract:** The global convergence of a recently proposed constant modulus (CM) and cross-correlation (CC)-based algorithm (CC-CMA) is studied in this paper. We first show the original analysis of global convergence of CC-CMA is incorrect. We then point out that the global convergent analysis of gradient stochastic algorithms including CC-CMA could be completed by solving a semi-algebraic set. By developing an optimal algorithm to examine the roots distribution a semi-algebraic set related with CC-CMA, we present that CC-CMA can converge globally if the parameter which mix the CM and CC terms is properly selected. Since our approach is quite general, it can be extended to the convergence analysis of any gradient stochastic algorithm. Simulation results confirm the theoretical analysis on the conditions of mixing parameter.

**Key-words:** Blind signal separation, constant modulus algorithm, cross-correlation, semi-algebraic set, discriminant variety, Gröbner bases.

[*] ng@deakin.edu.au
[†] School of Engineering and Technology, Deakin University, Geelong, VIC 3217, Australia. Tel +61 3 5227 1150, Fax 61 3 5227 2167
[‡] Daniel.Lazard@lip6.fr
[§] SALSA project - INRIA, CNRS and University of Paris VI
[¶] Fabrice.Rouillier@inria.fr
[‖] yxiang@deakin.edu.au

# Sur la détermination des paramètres de mélange de l'algorithme CC-CMA par l'étude d'ensembles semi-algébriques

**Résumé :** Ce rapport montre comment utiliser efficacement quelques outils de clacul symbolique pour assurer la convergence globale d'un algorithme récent d'optimisation (CC-CMA) de type gradient stochastique mélangeant des termes CM (module constant) et CC (inter-corrélation). Dans un premier temps, nous montrons que l'analyse originale de ce processus est incorecte puis établissons que l'étude de convergence se ramène à la résolution d'un système d'égalités et d'inégalités polynomiales d'épendant de paramètres. La description des solutions de ce système par une méthode formelle montre que le processus (CC-DMA) peut converger globalement dès lors que les paramètres fixant le mélange des termes CM (module constant) et CC (inter-corrélation) sont fixés correctement. Notre approche étant générale, elle peut a priori être étendue à l'analyse de convergence de tout algorithme de gradient stochastic.Enfin, nous proposons quelques simulations illustrant les résultats obtenus

**Mots-clés :** séparation de signaux, algorithme module constant, inter-corrélation, ensemble semi-algébrique, variété discriminante, bases de Gröbner

# 1 Introduction

The problem of blind signal separation (BSS) is of continuing interest in a wide range of fields such as wireless communications and signal processing applications. The basic objective of the BSS is to recover a set of source signals from a set of observations that are mixtures of the sources with no, or very limited knowledge about the mixture structure and source signals. To extract the original sources, many BSS algorithms have been proposed during the past decade [15]. Among these algorithms, the cross-correlation and constant modulus algorithm (CC-CMA), first reported in [21]-[22], appears to be the algorithm of choice due to its computational simplicity. The constant modulus (CM) term of the CC-CMA, which can be regarded as an extension to MIMO systems of CM algorithm in [14] and [31], aims to guarantee obtaining a single signal at each output of the separator. To prevent repeated retrieval of sources, a cross-correlation (CC) term is involved as the second term of CC-CMA to ensure all the retrieved sources are uncorrelated. The CM term and the CC term of the CC-CMA are weighted by a mixing parameter, which is a real positive number.

An important issue in CC-CMA algorithm is the global convergence analysis, which is first considered by Castedo *et al.* in [6]. This issue is important because the cost function proposed in the CC-CMA is not a quadratic form and may contain undesirable stationary points. If these undesirable points are local minima, the algorithm could be trapped in one of them. As a result, the CC-CMA would fail to separate source signals after it converges. By classifying all the stationary points into six groups and investigating the signs of principal minors of extended Hessian matrix at the stationary points in each group, Castedo *et al.* tried to prove that only the solutions in the group corresponding to desired separation are local minima if the normalized kurtosis of sources are less than two. However, as shown in Section II, such a conclusion is not true since one group of undesired stationary points can be local minima as well if there is no constraint on the mixing parameter.

It should be noted that the proper selection criterion on the mixing parameter can not be obtained by the method reported in [6] and [10]. This method is only feasible for the case where one of principal minors of the extended Hessian matrix is shown to be negative. For the concerned undesirable stationary points, the sign of principal minors will be uncertain unless further information about the distribution of these stationary points depending on the mixing parameter is available. Moreover, the existing results of the convergence analysis on CC-CMA for finite impulse response (FIR) channel (see [16] and [18]) also can not be applied to the studied problem, as they rely on the assumption that the channel and source signals are all real values. In this paper, in contrast, we will consider the case that the channel and sources take complex values. Besides the CC-CMA, there still exist some other BSS techniques which have been proved to be global convergent. The typical examples include the convergence analysis of multiuser kurtosis maximization (MUK) algorithm in [23] and hierarchical criteria for MIMO blind deconvolution in [30]. The analysis in [23] is based on a special property of MUK algorithm in which the updating of each row in matrix equalizer only depends on its previous row vectors. The analysis on hierarchical criteria for MIMO blind deconvolution relies on the hierarchical structure of cost function in [30]. Since these analyses exploit some properties which can not be expected in the CC-CMA, they are not feasible for our problem as well.

In this paper, we will complete the results of [6] by providing a constraint on the mixing parameter which then guarantees the global convergence of the CC-CMA. Different from the methods mentioned above, we address the problem by investigating the solutions of the semi-algebraic sets. Loosely speaking, a semi-algebraic set is the set of solutions of a system of polynomial equations and polynomial inequalities depending on variables which are either unknowns or parameters. In fact, the convergence analysis for many stochastic gradient algorithms can be completed by computing the points where the gradient of cost function vanishes and examining the positiveness of the principal minors of Hessian matrix at these points (see [5], [10], [11], [13], [19], [29]). Clearly, we can construct some semi-algebraic sets from these gradient equations and principal minors. By deriving a systematic method to solve semi-algebraic sets, we present a general frame for convergence analysis of a family of stochastic gradient algorithms, thus facilitating algorithm design.

Another appealing feature of our approach is the computation efficiency. In theory, determining the root distribution of a semi-algebraic system can be realized by some existing techniques such as the Cylindrical Algebraic Decomposition (CAD) and Comprehensive Gröbner bases method. However, these methods can not be employed for our problem since they are far from being efficient in practice. The computation of discriminant variety, an important concept in algebraic geometry which will be introduced in Section III, of the CAD [7] is obtained by considering all the polynomial equations and polynomial inequalities in a semi-algebraic set. Obviously, when the number of equations and inequalities in the studied semi-algebraic system becomes large, the computation burden of the CAD algorithm will be huge. To reduce the computation complexity, a partial CAD algorithm is proposed by [8]. However, it is still not an optimal algorithm since the discriminant variety obtained by this method depends on selecting proper projection strategy. As for the algorithms based on Comprehensive Gröbner bases(see [32], [33]), the computation also relies on an ad-hoc projection strategy. Thus, they are only efficient for some special cases. In this paper, we will develop a systematic approach to solve a semi-algebraic set with low computation complexity. Our algorithm is optimal in the sense that the discriminant variety it derives is a Zariski closure, which is the smallest subset of necessary variety. Hence, any unnecessary information will not be produced by our algorithm.

This paper is organized as follows. Section II formulates the problem. The necessary mathematic knowledge are summarized in Section III. The algorithm for determining the root distribution of semi-algebraic system is proposed in Section IV. Section V presents a selection criterion for the mixing parameter of the CC-CMA. Numerical simulation are provided in section VI to validate our results and section VII is devoted to the conclusion.

## 2 Problem Formulation

We consider that mutually independent sequences are transmitted through a MIMO linear memoryless channel. The system model takes the following form

$$\mathbf{x} = \mathbf{A}\mathbf{s} + \mathbf{n} \tag{1}$$

where $\mathbf{x}$ is a $N \times 1$ vector of observations, $\mathbf{A}$ denotes the $N \times K$ system channel, $\mathbf{s}$ represents a $K \times 1$ vector of transmitted symbols and $\mathbf{n}$ is the $N \times 1$ vector of Gaussian noise. Note that $N$ must be no less than $K$ to meet the channel invertibility condition. The objective of BSS is to select the proper weights of a separating matrix $\mathbf{W}$ with $K \times N$ dimension in such a way that each element in the output vector restores one of the different sources. The $i$th element of the output vector can be described as

$$y_i = \mathbf{w}_i^H \mathbf{x} \qquad i = 1 \dots K \tag{2}$$

where $\mathbf{w}_i^H$ is the $i$th row vector of matrix $\mathbf{W}$. The superscript $^H$ denotes the transpose conjugate operation. The CC-CMA algorithm minimizes the following cost function to perform source separation

$$J = \sum_{i=1}^{K} E[||y_i|^2 - 1|^2] + \frac{\alpha}{2} \sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} |E[y_i y_i^*]|^2 \tag{3}$$

where the mixing parameter $\alpha$ is a real positive number, $E[\cdot]$ is the expectation operator and $^*$ denotes conjugate.

Based on the assumption that the sources are independent, non-Gaussian, zero-mean, complex-valued signals with circular symmetry, the convergence analysis of the CC-CMA is considered by [6]. For the sake of simplicity, the analysis is restricted to a two-input two-output MIMO system under a noise-free environment. Therefore, the input-output relationship of such a system can be written as

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \tag{4}$$

where $g_{ij}$ corresponds to the overall response of the $i$th output to the $j$th source. Denote $k_i = E[|s_i|^4]/E[|s_i|^2]$ as the normalized kurtosis of $s_i$. One can easily find the cost function $J$ can also be expressed in terms of $k_i$ and $g_{ij}$ as

$$\begin{aligned} J \;=\; & k_1|g_{11}|^4 + k_2|g_{12}|^4 + 4|g_{11}|^2|g_{12}|^2 + k_1|g_{21}|^4 \\ & + k_2|g_{22}|^4 + 4|g_{21}|^2|g_{22}|^2 - 2|g_{11}|^2 - 2|g_{12}|^2 \\ & - 2|g_{21}|^2 - 2|g_{22}|^2 + \alpha(|g_{11}|^2|g_{21}|^2 + |g_{12}|^2|g_{22}|^2 \\ & + g_{11}g_{12}^*g_{21}^*g_{22} + g_{11}^*g_{12}g_{21}g_{22}^*) + 2. \end{aligned} \tag{5}$$

Taking the first derivative of (5) w.r.t. $g_{11}$, $g_{12}$, $g_{21}$ and $g_{22}$ yields the following equations

$$\begin{aligned}
\frac{\partial J}{\partial g_{11}} &= g_{11}^*(2k_1|g_{11}|^2 + 4|g_{12}|^2 - 2 + \alpha|g_{21}|^2) + \alpha g_{12}^* g_{21}^* g_{22} \\
\frac{\partial J}{\partial g_{12}} &= g_{12}^*(2k_2|g_{12}|^2 + 4|g_{11}|^2 - 2 + \alpha|g_{22}|^2) + \alpha g_{11}^* g_{21} g_{22}^* \\
\frac{\partial J}{\partial g_{21}} &= g_{21}^*(2k_1|g_{21}|^2 + 4|g_{22}|^2 - 2 + \alpha|g_{11}|^2) + \alpha g_{11}^* g_{12} g_{22}^* \\
\frac{\partial J}{\partial g_{22}} &= g_{22}^*(2k_2|g_{22}|^2 + 4|g_{21}|^2 - 2 + \alpha|g_{12}|^2) + \alpha g_{11} g_{12}^* g_{21}^*.
\end{aligned} \tag{6}$$

Obviously, all the stationary points of the CC-CMA are the roots of the above equations. These nonlinear equations contain multiple solutions which can be classified into six groups [6]. By investigating these groups respectively, Castedo *et al.* claimed the CC-CMA algorithm will be globally convergent if $k_i < 2$ since only the solutions in the group corresponding to desired separation are local minima. Such a conclusion is not true since one group of the undesired stationary points can also be local minima if there is no constraint on $\alpha$. The concerned group is *Group 6* in [6]. In this case, Each output of the separator extracts a linear combination of both sources, i.e., the four $g_{ij}$ are different from zero. To examine whether these undesired stationary points are local minima or not, one needs to check the positiveness of the following extended Hessian Matrix

$$\mathbf{H}_G J = \begin{bmatrix} \frac{\partial^2 J}{\partial g_{ij}\partial g_{kl}^*}\Big|_{i,j,k,l=1}^2 & \frac{\partial^2 J}{\partial g_{ij}\partial g_{kl}}\Big|_{i,j,k,l=1}^2 \\ \frac{\partial^2 J}{\partial g_{ij}^*\partial g_{kl}^*}\Big|_{i,j,k,l=1}^2 & \frac{\partial^2 J}{\partial g_{ij}^*\partial g_{kl}}\Big|_{i,j,k,l=1}^2 \end{bmatrix}. \tag{7}$$

From (6), we know that

$$\begin{aligned}
\frac{\partial^2 J}{\partial g_{11}\partial g_{11}^*} &= 2k_1|g_{11}|^2 - \alpha\frac{g_{11}g_{12}^*g_{21}^*g_{22}}{|g_{11}|^2} \\
\frac{\partial^2 J}{\partial g_{12}\partial g_{12}^*} &= 2k_2|g_{12}|^2 - \alpha\frac{g_{11}^*g_{12}g_{21}g_{22}^*}{|g_{11}|^2}.
\end{aligned} \tag{8}$$

Since $\frac{\partial^2 J}{\partial g_{11}\partial g_{11}^*}$ and $\frac{\partial^2 J}{\partial g_{12}\partial g_{12}^*}$ must be real, we have

$$g_{11}g_{12}^*g_{21}^*g_{22} = g_{11}^*g_{12}g_{21}g_{22}^* = \pm|g_{11}||g_{12}||g_{21}||g_{22}|. \tag{9}$$

It should be noted that only the positive case of (9) is considered by [6].

If $g_{11}g_{12}^*g_{21}^*g_{22} = g_{11}^*g_{12}g_{21}g_{22}^* = |g_{11}||g_{12}||g_{21}||g_{22}|$, it can be easily found that the determinant of the second upper left matrix of (7) takes the following form

$$\begin{aligned}
\Delta_2 &= det\begin{vmatrix} \frac{\partial^2 J}{\partial g_{11}\partial g_{11}^*} & \frac{\partial^2 J}{\partial g_{11}\partial g_{12}^*} \\ \frac{\partial^2 J}{\partial g_{12}\partial g_{11}^*} & \frac{\partial^2 J}{\partial g_{12}\partial g_{12}^*} \end{vmatrix} \\
&= 4|g_{11}|^2|g_{12}|^2(k_1k_2 - 4) - 2\alpha|g_{11}||g_{12}||g_{21}||g_{22}|(k_1\frac{|g_{11}|^2}{|g_{12}|^2} + k_2\frac{|g_{12}|^2}{|g_{11}|^2} + 2).
\end{aligned} \tag{10}$$

Clearly, $\Delta_2$ in this case will be negative if $k_1 < 2$ and $k_2 < 2$. Hence, $\mathbf{H}_G J$ will not be (semi)positive at the stationary points which make $g_{11}g_{12}^*g_{21}^*g_{22}$ positive.

If we consider the negative case of (9), the determinant of the second upper left matrix can be obtained as follows

$$\Delta_2 = 4|g_{11}|^2|g_{12}|^2(k_1k_2-4) + 2\alpha|g_{11}||g_{12}||g_{21}||g_{22}|(k_1\frac{|g_{11}|^2}{|g_{12}|^2} + k_2\frac{|g_{12}|^2}{|g_{11}|^2} + 2). \tag{11}$$

When $k_1 < 2$ and $k_2 < 2$, the first term of (11) will be negative. However, the value of $\Delta_2$ in this case is uncertain since the second term of (11) will always be positive. Moreover, one can find the sign of other principal minors of (7) can not be determined either for the case $g_{11}g_{12}^*g_{21}^*g_{22} = g_{11}^*g_{12}g_{21}g_{22}^* = -|g_{11}||g_{12}||g_{21}||g_{22}|$. Therefore, the positiveness of $\mathbf{H}_G J$ in this case can not be determined and the condition $k_1 < 2$ and $k_2 < 2$ are not sufficient to ensure that CC-CMA is globally convergent.

Naturally, one wants to find a range for $\alpha$ which makes (6) have roots satisfying $g_{11}g_{12}^*g_{21}^*g_{22} = g_{11}^*g_{12}g_{21}g_{22}^* = -|g_{11}||g_{12}||g_{21}||g_{22}|$ and $\mathbf{H}_G J$ will not be (semi)positive at these roots. To find the selection criterion on $\alpha$, we employ the method developed for solving semi-algebraic sets. As mentioned in Section I, a semi-algebraic set consists of polynomial equations and inequalities. Clearly, in our case, the equations originate from $\frac{\partial J}{\partial g_{11}} = 0$, $\frac{\partial J}{\partial g_{12}} = 0, \frac{\partial J}{\partial g_{21}} = 0$ and $\frac{\partial J}{\partial g_{22}} = 0$ respectively. The equations in the algebraic set can be further written as follows by multiplying $g_{ij}$ by $\frac{\partial J}{\partial g_{ij}}$ respectively

$$\begin{aligned}
|g_{11}|(2k_1|g_{11}|^2 + 4|g_{12}|^2 - 2\alpha|g_{21}|^2) - \alpha|g_{12}||g_{21}||g_{22}| = 0\\
|g_{12}|(2k_2|g_{12}|^2 + 4|g_{11}|^2 - 2\alpha|g_{22}|^2) - \alpha|g_{11}||g_{21}||g_{22}| = 0\\
|g_{21}|(2k_1|g_{21}|^2 + 4|g_{22}|^2 - 2\alpha|g_{11}|^2) - \alpha|g_{11}||g_{12}||g_{22}| = 0\\
|g_{22}|(2k_2|g_{22}|^2 + 4|g_{21}|^2 - 2\alpha|g_{12}|^2) - \alpha|g_{11}||g_{12}||g_{21}| = 0.
\end{aligned} \tag{12}$$

Moreover, we have the following inequalities

$$\begin{aligned}
0 < k_1 < 2, 0 < k_1 < 2, \alpha > 0\\
|g_{11}| > 0, |g_{12}| > 0, |g_{21}| > 0, |g_{22}| > 0.
\end{aligned} \tag{13}$$

Our problem is to find the necessary and sufficient conditions on the parameters $k_1$, $k_2$ and $\alpha$ such that the algebraic set, composed by equations (12) and inequalities (13), has solutions which make $\mathbf{H}_G J$ not be (semi)positive. It should be noted that such a problem can be reduced to a simplified version for wireless communication since different users normally share the same statistical properties, i.e., $k_1 = k_2$. Without loss of generality, we further assume $k_1 = k_2 = 1$. In this case, M-ary phase shifting keying (MPSK) modulation scheme is used to transmit the symbols. Thus, the studied problem in this paper can be described as determining the range of $\alpha$ which makes the following semi-algebraic set

$$\left\{\begin{array}{c}
|g_{11}|(2|g_{11}|^2 + 4|g_{12}|^2 - 2\alpha|g_{21}|^2) - \alpha|g_{12}||g_{21}||g_{22}| = 0\\
|g_{12}|(2|g_{12}|^2 + 4|g_{11}|^2 - 2\alpha|g_{22}|^2) - \alpha|g_{11}||g_{21}||g_{22}| = 0\\
|g_{21}|(2|g_{21}|^2 + 4|g_{22}|^2 - 2\alpha|g_{11}|^2) - \alpha|g_{11}||g_{12}||g_{22}| = 0\\
|g_{22}|(2|g_{22}|^2 + 4|g_{21}|^2 - 2\alpha|g_{12}|^2) - \alpha|g_{11}||g_{12}||g_{21}| = 0\\
\alpha > 0, |g_{11}| > 0, |g_{12}| > 0, |g_{21}| > 0, |g_{22}| > 0
\end{array}\right. \tag{14}$$

have real solutions. In the mean time, all these solutions make $\mathbf{H}_G J$ not be (semi)positive.

# 3 Necessary Mathematical Knowledge

According to the above section, we know that the first problem needs to be solved is to determine the root distribution of a parametric system (14). We address such a problem by investigating the number of real roots of the following semi-algebraic set

$$\mathcal{S}: \begin{cases} p_1(X,\alpha)=0 \\ p_2(X,\alpha)=0 \\ \cdots \\ p_s(X,\alpha)=0 \\ f_1(X,\alpha)>0 \ldots f_l(X,\alpha)>0 \end{cases} \tag{15}$$

where $X=\{X_1,\ldots,X_n\}$ is the set of indeterminates, $\alpha$ is a unique parameter, $p_i$ and $f_i$ are the polynomials in terms of $X$ and $\alpha$. For our specific case, $X_1=|g_{11}|, X_2=|g_{12}|, X_3=|g_{22}|, X_4=|g_{21}|$, $p_i$ and $f_i$ are the polynomials in terms of $X$ and $\alpha$ defining the equations and inequalities of (14) respectively It should be noted that the first derivative of many stochastic gradient algorithms under some practical constraints can be modeled by system (15) (see [5], [10], [11], [13], [19], [29]). As a result, developing a general method to determine the root distribution of semi-algebraic set (15) can provide a uniform frame for analyzing the convergence of a family of stochastic gradient algorithms.

We do not give any proof in this section. Most of them may be found in many places, and especially in [9]. For the results which do not appear there, we will give explicit references.

## 3.1 Mathematical background

In the sequel, we will borrow some elements from algebraic geometry and cumulative algebra to solve system (15). To facilitate illustrating our methods more easily, we introduce a minimal dictionary at first. For such a purpose, an essential structure is the ideal.

**Definition 1** *Let $k$ be a field, and let $P_1,\cdots,P_s$ be the polynomials in $k[X,\alpha]$. Then we call*

$$\langle P_1,\cdots,P_s\rangle=\{\sum_{i=1}^{s}h_iP_i : h_1,\cdots,h_s\in\mathbb{R}[X,\alpha]\} \tag{16}$$

*the ideal generated by $P_1,\cdots,P_s$.*

We denote by $\mathcal{E}=\langle p_1,\ldots,p_s\rangle$ the ideal generated by the polynomials defining the equations in (15) and by $\mathcal{F}=\{f_1,\ldots,f_l\}$ the set of polynomials defining the inequalities in the inequalities of (15). The geometrical objects to be studied are the variety of the ideal $\mathcal{E}$ and the semi-algebraic set consisting in the points of this variety which satisfy the inequalities. Moreover, assuming that $k=\mathbb{Q}$, two set of varieties will be studied in this paper which include the complex variety (the set of complex zeroes of a given ideal) and the real variety (the set of real zeros of an ideal).. Both of them are defined independently from the chosen set of generators of the ideal.

**Definition 2** *Let $P_1, \cdots, P_s$ be polynomials in $\mathbb{Q}[X, \alpha]$. Then we set*

$$V(P_1, \cdots, P_s) = \{X \in \mathbb{C}^{n+1} : P_i(X, \alpha) = 0, \quad 1 \leq i \leq s\}. \tag{17}$$

*We call $V(P_1, \cdots, P_s)$ as the variety defined by $P_1, \cdots, P_s$. The real variety will be denoted by $V(P_1, \cdots, P_s) \cap \mathbb{R}^{n+1}$.*

Another important concept which needs to be introduced is *discriminant variety.* Loosely speaking, a discriminant variety, denoted by $W_D$, is an algebraic variety (systems of algebraic equations depending only on the parameters) defining a partition of parameter's space into subsets which are

- the discriminant variety $W_D$ itself, and
- open connected disjoint subsets $\mathcal{U}_1, \cdots, \mathcal{U}_r$ of parameters' space which do not insect the discriminant variety and such that any solution of (15) which the parameters lying in some $\mathcal{U}_i$ belongs to the image of an analytic function of $\mathcal{U}_i$ into the solutions of (15).

A more precise definition of discriminant variety can be found in [17]. Normally, the discriminant variety is defined in the complex case, i.e. one is interested with the study of the complex roots of the system $\tilde{\mathcal{S}}$ obtained by replacing the inequalities in $\mathcal{S}$ with inequations. But the definitions commute with the intersection with the real space. One can thus first define the discriminant variety $W_D$ for the complex system $\tilde{\mathcal{S}}$ and then get the restriction $W_D \cap \mathbb{R}$ as a discriminant variety of $\mathcal{S}$ .

A very interesting property of discriminant varieties is that, if $u$ and $v$ are two vectors of parameters which belong to the same $\mathcal{U}_i$, the specialized systems $\mathcal{S}_{\alpha=u}$ and $\mathcal{S}_{\alpha=v}$ have exactly the same number of real roots. Based on this property, we know that one key step in solving our problem is to compute a discriminant variety $W_D$ of $\mathcal{S}$. Since there is only one parameter ($\alpha$) in our studied system, determining $W_D$ of $\mathcal{S}$, or more precisely counting the number of solutions of the system w.r.t. $\alpha$ remains to

- set $\alpha_0 = 0$ and $\alpha_{r+1} = \infty$ and compute real numbers $\alpha_1, \ldots, \alpha_r$ such that over $]\alpha_i, \alpha_{i+1}[, i = 0 \ldots r$, $V(\mathcal{S}) \cap \mathbb{R}$ is an analytic covering of $]\alpha_i, \alpha_{i+1}[$ for the projection on the $\alpha$-axis, i.e., $V(\mathcal{S}) \cap \mathbb{R}$ is the union of analytic branches which do not intersect over, $]\alpha_i, \alpha_{i+1}[$. Note that this property induces that the system has a constant number of real solutions over each interval $]\alpha_i, \alpha_{i+1}[$.
- take any rational number $\beta_i \in ]\alpha_i, \alpha_{i+1}[$ for $i = 1 \ldots r$, and count the number of real roots of $V(\mathcal{S}) \cup \{\alpha = \beta_k\}$, which is the constant number of real roots of all systems $V(\mathcal{S}) \cup \{\alpha = \gamma_i\}$ with $\gamma_i \in ]\alpha_i, \alpha_{i+1}[$.
- for each $\alpha_i$, $i = 1 \ldots r$, solve the system $V(\mathcal{S}) \cup \{\alpha = \alpha_i\}$.

Now, we are in the position to present a method to calculate $W_D$. For simplicity, we first consider $W_D$ of $\mathcal{E}$, i.e., we do not consider the inequalities in (15) at this stage. Since

$W_D$ is only related to the parameter space (only related to $\alpha$ in our case), we introduce the following projection mapping operation

$$\Pi_\alpha : \mathbb{C}^{(n+1)} \longrightarrow \mathbb{C} \tag{18}$$

which sends $(\alpha, X_1, \cdots, X_n)$ to $\alpha$. Moreover, we denote by $\Pi_\alpha^{-1}$ the inverse projection on the parameter space $(\alpha) \longrightarrow (\alpha, X_1, \cdots, X_n)$. According to [17], $W_D$ of $\mathcal{E}$ can be obtained as follows

$$W_D = O_\infty \cup \ O_c \cup \{0, +\infty\} \tag{19}$$

where $O_\infty$ is the set of $\alpha \in \mathbb{R}$ such that $\Pi_\alpha^{-1}(\alpha) \bigcap \mathrm{V}(\mathcal{E})$ is not compact for any compact neighborhood $\mathcal{U}$ of $\alpha$ and $O_c$ is the set of real critical values of $\Pi_\alpha$ restricted to $\mathrm{V}(\mathcal{E})$ (from the pure algebraic point of view, this includes the projections of singular points). In other words, $O_\infty$ modelizes the phenomena "roots going to infinity" when the parameter varies while $O_c$ modelizes "critical values and projections of singular points". Classical mathematical results (see [20] for $O_\infty$ and Sard's semi-algebraic theorem in [1] for $O_c$) show that these two sets of points are finite in general and we will see later that it is the case for our problem.

Let us now consider the full semi-algebraic set $\mathcal{S}$ which includes the inequalities in (15). According to the above results, one can decompose $\mathrm{V}(\mathcal{E})$ as points and continuous branches which do not intersect. In the following, we use the fact that the sign of a given polynomial (for example $f_1$) will not be constant on such a branch if and only if $f_i$ vanishes at some point. Let us define $O_\infty \cup O_c = \{\alpha'_0, \ldots, \alpha'_{k+1}\}$. Over each interval $]\alpha'_i, \alpha'_{i+1}[$, either $f$ is identically null at each point of a given branch, or it vanishes at a finite number of points or it never vanishes. We suppose that $f$ vanishes at most at a finite number of points, which remains to suppose that $\mathrm{V}(\mathcal{E}) \cap \mathbb{R}^5 \cap \{x \in \mathbb{R}^5, f = 0\}$ is a finite set of points (we will see how to get rid of this condition on our problem in next section). Thus, there exists a finite number of reals $\omega_1, \ldots, \omega_t$ such that $\cup_{i=1}^t \mathrm{V}(\mathcal{E}) \cap \mathbb{R}^5 \cap \{\alpha = w_i\}$ contains $\mathrm{V}(\mathcal{E}) \cap \mathbb{R}^5 \cap \{f_1 = 0 \vee \ldots \vee f_l = 0\}$. If we take $\{\alpha_0, \ldots, \alpha_{r+1}\} = O_c \cup O_\infty \cup \{0, +\infty\} \cup \{\omega_1, \ldots, \omega_s\}$, the semi-algebraic system $\mathcal{S}$ then has a constant finite number of points over each interval $]\alpha_i, \alpha_{i+1}[$. Therefore, the discriminant variety $W_D$ of $\mathcal{S}$ can be obtained by

$$W_D = O_\infty \cup \ O_c \cup \{0, +\infty\} \cup \{\omega_1, \ldots, \omega_s\}. \tag{20}$$

## 3.2 Algorithmic background

From section 3.1, one can see that the main difficulty is to compute explicitly $O_\infty$, $O_c$ and $w_1, \ldots, w_s$. Moreover, we know that eliminating the indeterminates $X$ from $\mathcal{S}$ is a key ingredient of computing $W_D$. In this section, we resort to the Gröbner basis to realize such computations. Here, we first briefly summarize some known basic results about Gröbner bases and their applications to elimination theory and solving zero-dimensional systems. A complete introduction of Gröbner bases can be found in [9], [4] and [2].

### 3.2.1 Gröbner bases

A Gröbner basis of an ideal $I$ is a computable generator set of $I$ with good algorithmical properties and defined with respect to a monomial ordering. In this paper, we will use the two following orderings and some others which will be defined later.

- *lexicographic order*: (Lex)

$$\begin{array}{l} X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n} <_{\mathrm{Lex}} X_1^{\beta_1} \cdot \ldots \cdot X_n^{\beta_n} \\ \Leftrightarrow \exists i_0 \leq n \quad , \quad \left\{ \begin{array}{l} \alpha_i = \beta_i, \quad \text{for } i = 1, \ldots, i_0 - 1, \\ \alpha_{i_0} < \beta_{i_0} \end{array} \right. \end{array} \tag{21}$$

- *degree reverse lexicographic order (DRL)*:

$$\begin{array}{l} X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n} <_{\mathrm{DRL}} X_1^{\beta_1} \cdot \ldots \cdot X_n^{\beta_n} \\ \Leftrightarrow X_0^{\sum_k \alpha_k} \cdot X_1^{-\alpha_n} \cdot \ldots \cdot X_n^{-\alpha_1} <_{\mathrm{Lex}} X_0^{\sum_k \beta_k} \cdot X_1^{-\beta_n} \cdot \ldots \cdot X_n^{-\beta_1}. \end{array} \tag{22}$$

Let us define the mathematical object "Gröbner basis".

**Definition 3** *For any n-uple $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, let denote by $X^\mu$ the monomial $X_1^{\mu_1} \cdot \ldots \cdot X_n^{\mu_n}$. Given an admissible monomial ordering $<$ and $P = \sum_{i=0}^r a_i X^{\mu^{(i)}}$ a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$, we define* $\mathrm{LM}(P, <) = \max_{i=0\ldots r\,,\,<} X^{\mu^{(i)}}$ *which is the* leading monomial *of $P$ w.r.t. $<$;* $\mathrm{LC}(P, <) = a_i$ *with* $\mathrm{LM}(P, <) = X^{\mu^{(i)}}$ *which is the* leading coefficient *of $P$ w.r.t. $<$ and* $\mathrm{LT}(P, <) = \mathrm{LC}(P, <)\,\mathrm{LM}(P, <)$ *which is the* leading term *of $P$ w.r.t $<$.*

**Definition 4** *A set of polynomials $G$ is a Gröbner basis of an ideal $I$ w.r.t to a monomial ordering $<$ if for all $f \in I$ there exists $g \in G$ such that $LM(g, <)$ divides $LM(f, <)$.*

Given any admissible monomial ordering $<$, one can easily extend the classical Euclidean division to *reduce* a polynomial $p$ by a set of polynomials $F$, performing the reduction w.r.t to each polynomial of $F$ until getting an expression which can not be further reduced. Let denote such a function by $\texttt{Reduce}(p, F, <)$ (reduction of the polynomial $p$ w.r.t $F$). Unlike in the univariate case, the result of such a process is not canonical unless $F = G$ is a Gröbner basis.

**Theorem 1** *[9] Let $G$ be a Gröbner basis of an ideal $I \subset \mathbb{Q}[X_1, \ldots, X_n]$ for a fixed ordering $<$. Then,*

*(i) a polynomial $p \in \mathbb{Q}[X_1, \ldots, X_n]$ belongs to $I$ if and only if* $\texttt{Reduce}(p, G, <)$,

*(ii)* $\texttt{Reduce}(p, G, <)$ *does not depend on the order in which the reductions by polynomials in $G$ are done. Thus, this is a canonical representation of the polynomials which are equivalent to $p$ modulo $I$.*

Gröbner bases are computable objects. The most popular method for computing them is Buchberger's algorithm [3]. It has several variants and is implemented in most of computer algebraic software such as Maple or Mathematica. For difficult computations, one will prefer dedicated software such as FGb developed by J.C. Faugère [12].

### 3.2.2 Elimination or block orderings

We pay a particular attention to Gröbner bases with respect to elimination or block orderings (defined below) since they provide a way of *eliminate* some variables from the system. Especially the discriminant variety, which is defined by equations depending only from the parameters is efficiently obtained by Gröbner basis computations for an ordering eliminating the $X_i$.

**Definition 5** *Given two monomial orderings $<_U$ (w.r.t. the variables $U_1, \dots, U_d$) and $<_X$ (w.r.t. the variables $X_{d+1}, \dots, X_n$), a* block ordering *$<_{U,X}$ is defined as follows : given two monomials $m$ and $m'$, then $m <_{U,X} m'$ if and only if either $m_{|U_1=1,\dots,U_d=1} <_X m'_{|U_1=1,\dots,U_d=1}$ or ($m_{|U_1=1,\dots,U_d=1} = m'_{|U_1=1,\dots,U_d=1}$ and $m_{|X_{d+1}=1,\dots,X_n=1} <_U m'_{|X_{d+1}=1,\dots,X_n=1}$). We say that such an ordering* eliminates *$X_{d+1}, \dots, X_n$.*

The lexicographical ordering such $X_1 < \dots < X_n$ is a block ordering for any $1 < i < n$, which eliminates $X_{i+1}, \dots, X_n$. However, this ordering is not recommended for elimination because the computation is usually much harder than with block orderings such both $<_U$ and $<_X$ are DRL orderings.

Two important applications of elimination orderings are the *projections* and *localizations*, which can be summarized in Proposition 1 and 2. To facilitate the illustration, the following notation is needed. Given any subset $\mathcal{V}$ of $\mathbb{C}^d$ ($d$ is an arbitrary positive integer), $\overline{\mathcal{V}}$ is its Zariski closure which is the smallest subset of $\mathbb{C}^d$ containing $\mathcal{V}$. If $\mathcal{V}$ is a constructible set (i.e. it may be defined by equations and inequations), then $\overline{\mathcal{V}}$ is also the closure for the usual topology. This will be always the case in the following.

**Proposition 1** *[4] Let $G$ be a Gröbner basis of an ideal $I \subset \mathbb{Q}[U, X]$ w.r.t. a block ordering $<_{U,X}$, then $G \bigcap \mathbb{Q}[U]$ is a Gröbner basis of $I \bigcap \mathbb{Q}[U]$ w.r.t. $<_U$. Moreover, if $\Pi_U : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ denotes the canonical projection on the coordinates $U$, then $V(I \cap \mathbb{Q}[U]) = V(G \cap \mathbb{Q}[U]) = \overline{\Pi_U(V(I))}$.*

**Proposition 2** *[9] Let $I \subset \mathbb{Q}[X]$ and $T$ be a new indeterminate, then $\overline{V(I) \setminus V(f)} = V((I + \langle Tf - 1\rangle) \bigcap \mathbb{Q}[X])$. If $G' \subset \mathbb{Q}[X, T]$ is a Gröbner basis of $I + \langle Tf - 1\rangle$ w.r.t a block ordering $<_{X,T}$, then $G' \bigcap \mathbb{Q}[X]$ is a Gröbner basis of $I : f^\infty := (I + \langle Tf - 1\rangle) \bigcap \mathbb{Q}[X]$ w.r.t. $<_X$. The variety $\overline{V(I) \setminus V(f)}$ and the ideal $I : f^\infty$ are usually called the localization of $V(I)$ and $I$ by $f$.*

### 3.2.3 Certified solutions of zero-dimensional systems

Zero-dimensional systems are polynomial systems with a finite number of complex solutions. The following theorem shows whether we can detect that a system is zero dimensional or not by computing a Gröbner base for any monomial ordering.

**Theorem 2** *[2] Let $G = \{g_1, \dots, g_l\}$ be a Gröbner basis of a system $S = \{P_1, \dots, P_s\} \in \mathbb{Q}[X_1, \dots, X_n]^s$, for an ordering $<$. The following two properties are equivalent:*

- *For all index $i$, $i = 1 \dots n$, there exists a polynomial $g_j \in G$ and a positive integer $n_j$ such that $X_i^{n_j} = LM(g_j, <)$;*
- *The system $\{P_1 = 0, \dots, P_s = 0\}$ has a finite number of solutions in $\mathbb{C}^n$ (i.e. it is zero-dimensional).*

If $S$ is zero-dimensional, then according to Theorem 2, only a finite number of monomials $m \in \mathbb{Q}[X_1, \dots, X_n]$ are not reducible modulo $G$ (this means that $\texttt{Reduce}(m, G, <) = m$). This implies that a system is zero-dimensional if and only if $\mathbb{Q}[X_1, \dots, X_n]/I$ is a $\mathbb{Q}$-vector space of finite dimension. When a Gröbner basis $G$ is known, a basis of this vector space is given by the monomials which are not reducible by $G$ and the result of $\texttt{Reduce}(f, G, <)$ is the expression on this basis of the image of $f$ in $\mathbb{Q}[X_1, \dots, X_n]/I$.

**Theorem 3** *[9] Let $S = \{P_1, \dots, P_s\}$ be a set of polynomials with $p_i \in \mathbb{Q}[X_1, \dots, X_n], \forall i = 1 \dots s$, and suppose that $G$ is a Gröbner basis of $\langle S \rangle$ w.r.t any monomial ordering $<$, which satisfy the equivalent conditions of Theorem 2. Then, we have*

- *$\mathbb{Q}[X_1, \dots, X_n]/I = \{\ \texttt{Reduce}\ (p, G, <), p \in I\}$ is a vector space of finite dimension;*
- *$\mathcal{B} = \{t = X_1^{e_1} \cdot X_n^{e_n},\ \ (e_1, \dots, e_n) \in \mathbb{N}^n |\ \ \texttt{Reduce}(t, G, <) = t\} = \{w_1, \dots, w_D\}$ is a basis of $\mathbb{Q}[X_1, \dots, X_n]/I$ as a $\mathbb{Q}$-vector space;*
- *$D = \sharp\mathcal{B}$ (the number of elements in $\mathcal{B}$) is exactly the number of elements of complex zeroes of the system $\{P_1 = 0, \dots, P_s = 0\}$ counted with multiplicities.*

Thus, when a polynomial system is known to be zero-dimensional, one can switch to linear algebra methods to get information about its roots. Once a Gröbner basis is known, a basis of $\mathbb{Q}[X_1, \dots, X_n]/I$ can easily be computed according to Theorem 3.

For any polynomial $q \in \mathbb{Q}[X_1, \dots, X_n]$, the decomposition $\overline{q} = \texttt{Reduce}\ (q,G,<) = \sum_{i=1}^{D} a_i w_i$ is unique (see Theorem 1). We denote by $\vec{q} = [a_1, \dots, a_D]$ the representation of $\overline{q}$ in the basis $\mathcal{B}$. For example, the matrix w.r.t. $\mathcal{B}$ of the linear map

$$m_q \begin{pmatrix} \mathbb{Q}[X_1, \dots, X_n]/I & \longrightarrow & \mathbb{Q}[X_1, \dots, X_n]/I \\ \vec{p} & \longrightarrow & pq \end{pmatrix} \tag{23}$$

can be explicitly computed since its columns are the vectors $\overrightarrow{qw_i}$. One can then apply the following well-known theorem

**Theorem 4** *[2] The eigenvalues of $m_q$ are exactly the $q(\alpha)$ where $\alpha \in V_{\mathbb{C}}(S)$.*

According to Theorem 4, the $i$-th coordinate of all $\alpha \in V_{\mathbb{C}}(S)$ can be obtained from $M_{X_i}$ eigenvalues but the issue of finding all the coordinates of all the $\alpha \in V_{\mathbb{C}}(S)$ from $M_{X_1}, \dots, M_{X_n}$ eigenvalues is neither explicit nor straightforward and often numerically unstable.

**The Rational Univariate Representation** The Rational Univariate Representation (RUR) is, from the end-user point of view, the simplest way to symbolically represent the roots of a zero-dimensional system without losing information since one can get all the information on the roots of the system by solving univariate polynomials [26].

Given a zero-dimensional system $I$, a RUR of $\mathrm{V}(I)$ has the following shape

$$f_t(T) = 0, X_1 = \frac{g_{t,X_1}(T)}{g_{t,1}(T)}, \ldots, X_n = \frac{g_{t,X_n}(T)}{g_{t,1}(T)} \tag{24}$$

where $f_t, g_{t,1}, g_{t,X_1}, \ldots, g_{t,X_n} \in \mathbb{Q}[T]$, $T$ is a new variable. The RUR defines a bijection between the roots of $\mathcal{F}$ and those of $f_t$ preserving the multiplicities and the real roots

$$\begin{array}{ccc} \mathrm{V}(\mathcal{S})(\cap\mathbb{R}) & \approx & \mathrm{V}(f_t)(\cap\mathbb{R}) \\ \alpha = (\alpha_1, \ldots, \alpha_n) & \rightarrow & t(\alpha) \\ (\frac{g_{t,X_1}(t(\alpha))}{g_{t,1}(t(\alpha))}, \ldots, \frac{g_{t,X_n}(t(\alpha))}{g_{t,1}(t(\alpha))}) & \leftarrow & t(\alpha). \end{array} \tag{25}$$

To compute a RUR, one has to solve the following two problems:

- find a separating element $t$, and
- given any polynomial $t$, compute a RUR-Candidate $f_t, g_{t,1}, g_{t,X_1}, \ldots, g_{t,X_n}$ such that if $t$ is a separating polynomial, then the RUR-Candidate is a RUR.

According to [26], a RUR-Candidate can be explicitly computed when we know a suitable representation of $\mathbb{Q}[X_1, \ldots, X_n]/I$, which can be summarized as follows

- $f_t = \sum_{i=0}^{D} a_i T^i$ is the characteristic polynomial of $m_t$. Let us denote by $\overline{f_t}$ its square-free part.
- for any $v \in \mathbb{Q}[X_1, \ldots, X_n]$, $g_{t,v} = g_{t,v}(T) = \sum_{i=0}^{d-1} Trace(m_{vt^i}) H_{d-i-1}(T)$, $d = \deg(\overline{f_t})$ and $H_j(T) = \sum_{i=0}^{j} a_i T^{i-j}$

In [26], a strategy is proposed to compute a RUR for any system from a Gröbner basis for any ordering.

**From formal to numerical solutions** Computing a RUR reduces the resolution of a zero-dimensional system to solving a polynomial with one variable ($f_t$) and to evaluating $n$ rational fractions ($\frac{g_{t,X_i}(T)}{g_{t,1}(T)}, i = 1 \ldots n$) at the roots. The next task is thus to compute all the real roots of the system, providing a numerical approximation with an arbitrary precision of the coordinates.

The isolation of the real roots of $f_t$ can be done using the algorithm proposed in [28]. The output will be a list $l_{f_t}$ of intervals with rational bounds such that for each real root $\alpha$ of $f_t$, there exists a unique interval in $l_{f_t}$ which contains $\alpha$. The second step consists of refining each interval in order to ensure that it does not contain any real root of $g_{t,1}$. Since $f_t$ and $g_{t,1}$ are co-prime, this computation is easy. Then, we can ensure that the rational functions can be evaluated by using interval arithmetics without any cancelation of the denominator. The last evaluation is performed by using multi-precision arithmetics (MPFI package - [27]). Moreover, the rational functions defined by the RUR are stable under numerical evaluation even if their coefficients are huge rational numbers. Thus, the isolation of the real roots does not involve huge compaction burden. To increase the precision of the result, it is only necessary to decrease the length of the intervals in $l_{f_t}$ which can be easily done by bisection or using a certified Newton's algorithm. Note that it is quite simple to certify the sign of the coordinates.

**Signs of polynomials at the roots of a system** Due to the existence of inequalities in semi-algebraic system, it is important to develop a method computing the sign of given multivariate polynomials at the real roots of system (15) if it is zero-dimensional. Instead of *plugging* straightforwardly the formal coordinates provided by the RUR into the $f_i$, we better extend the RUR by computing rational functions $h_{t,j}$ which coincide with the $f_i$ at the roots of $I$. Precisely, using the notations 25, $f_i(\alpha_1, \ldots, \alpha_n) = h_{t,j}(t(\alpha_1, .., \alpha_n))$. This can be simply done by using the general formula $h_{t,j} = \sum_{i=0}^{D-1} Trace(f_j t^i) H_{D-i-1}(T)$ in [26]. One can directly compute the $Trace(f_j t^i)$ by reusing the computations already done if the RUR has already been computed. Hence, it is not more costly to compute the extended RUR than the classical one.

# 4 Computation of the roots distribution

The objective of this section is to prove the following result.

**Theorem 5** *If denote $\beta = \{X_1 = X_2 = X_3 = X_4 = \frac{1}{\sqrt{3}}\}$, we will have*

- *for $0 < \alpha < 1$ the system (14) has 5 solutions including $(\alpha, \beta)$;*
- *for $\alpha = 1$, the system (14) has 3 isolated points including $\beta$ and a infinite number of solutions which lies on a semi-algebraic curve defined by $X_1 = X_3, X_2 = X_4, X_3 = \sqrt{\frac{2-3*X_4^2}{3}}, X_4^2 > 2/3$;*
- *for $1 < \alpha < \infty$ the only solution for system (14) is $(\alpha, \beta)$.*

In order to use efficiently the properties of Gröbner basis introduced in section 3.2.1, we introduce the following specific monomial orderings.

**Notation 1** *Let $<_X$ be a DRL ordering in (22) for the monomials depending on the variables $X$, $<_{\alpha,X} = (<, <_X)$ will denote the product of orderings (see definition 5) $\alpha <_{\alpha,X} X_i$ for all $X_i \in X$ and $X_i <_{\alpha,X} X_j$ if and only if $X_i <_X X_j$ for all $X_i, X_j \in X$.*

As described in section 3.1, $O_c$ is the set of critical values of the restriction to $V \cap \mathbb{R}^5$ of the projection on the $\alpha$-axis or, equivalently, of the projection on the $\alpha$-axis of the critical points of the restriction to $V \cap \mathbb{R}^5$ of the projection on the $\alpha$-axis. Let's denote by $\mathrm{Jac}_X$

the Jacobian determinant w.r.t $X$ of $\mathcal{E}$. The critical points of the projection on the $\alpha$-axis are included in the solutions of the system $\mathcal{E}_c = \{\text{Jac}_X(\mathcal{E}), g = 0, g \in \mathcal{E}\}$. It appears that the system defining $\mathcal{E}_c$ is zero-dimensional. Since the number of polynomials in $\mathcal{E}$ equals the number of indeterminates, the critical points are exactly the roots of this system (more details about such situations can be founded in [17]). Thus, by computing a Gröbner basis of $\mathcal{E}_c$ w.r.t. $<_{\alpha,X}$ and applying Proposition 1, one obtains $O_c$ as the set of real zeros of a unique polynomial $P_c \in \mathbb{Q}[\alpha]$. For our system, we get $P_c = (\alpha-1)(\alpha-2)(\alpha-3)(\alpha+1)$.

In the same way, one can compute $P_{\mathcal{F}} \in \mathbb{Q}[\alpha]$ by eliminating the variables $X$ in the system $\mathcal{E}_{\mathcal{F}} = \{\prod_{f\in\mathcal{F}} f = 0, g = 0, g \in \mathcal{E}\}$ (see Proposition 1). We first obtain $P_{\mathcal{F}} = 0$, which means that some of the polynomials of $\mathcal{F}$ vanish on a entire (complex) component of V. Thus, we can localize $\mathcal{E}$ at $\prod_{f\in\mathcal{F}} f$ and obtain a system $\mathcal{E}'$ whose zeros are $\overline{\mathrm{V} \setminus \{x \in \mathbb{C}^5, f = 0, f \in \mathcal{F}\}}$ by Proposition 1 and 2. This variety represents the smallest algebraic variety containing all the branches of V (it is thus contained in V) for which none of the polynomials of $\mathcal{F}$ is identically null. Then, we compute $P_{\mathcal{F}}$ by using $\mathcal{E}'$ instead of $\mathcal{E}$ and obtain $P_{\mathcal{F}} = \alpha(\alpha-3)(\alpha-1)(\alpha-2)(\alpha+1)$.

The explicit computation of a finite set containing $O_\infty$ can be done using classical results from [9] or [4]. One can first compute a Gröbner basis $G$ of $I$ for $<_{\alpha,X}$ and then consider all the polynomials $LC(g, <_X), g \in G$ (which belong to $\mathbb{Q}[\alpha]$). $O_\infty$ as well as a part of $O_c$ is included in the union of the roots of these univariate polynomials , which yields some extraneous points with no geometrical meaning. Different with these classical methods, a more efficient approach is introduced as follows which yields less computed points.

**Theorem 6** *Let $G$ be a reduced Gröbner basis of any ideal $I$ whose zero set is $V$ w.r.t. a block ordering $<_{\alpha,X}$ . Here $<_X$ is the Degree Reverse Lexicographic ordering s.t. $X_1 < \ldots < X_n$. We define $g_i^\infty = gcd\{LC(g, <_X) \quad | \quad g \in G \quad , \quad \exists m \geq 0, \quad LM(g, <_X) = X_i^m\}$. Then,*

- *$O_\infty = \bigcup_{i=1}^n V(g_i^\infty) \cap \mathbb{R}$, where $V(g_i^\infty)$ denotes the (complex) zero set of $g_i^\infty$.*

The proof of this theorem appears in [17] which is based on the properties of the special monomial ordering.

Note that since $O_\infty = \mathrm{V}(\prod_{i=d^1}^n g_i^\infty)$, one can define $O_\infty$ as the set of real zeroes of a univariate polynomial $P_\infty \in \mathbb{Q}[\alpha]$. For our problem, we obtain $P_\infty = \alpha(\alpha-3)(\alpha-1)(\alpha+3)(\alpha+1)$. Let denote by $\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = 2, \alpha_3 = 3$ the real points of the discriminant variety and introduce $\alpha_4 = +\infty$. Based on the previous computation on $P_c, P_{\mathcal{F}}$ and $P_\infty$, we can find that system $\mathcal{S}$ has a constant finite number of real roots over each $]\alpha_i, \alpha_{i+1}[, i = 0..3$ or, equivalently, for each $i = 0\ldots3$, the systems $\mathcal{S} \cup \{\alpha = \gamma\}$ have a constant number of real roots $\forall\gamma \in ]\alpha_i, \alpha_{i+1}[$. Moreover, it has a finite number of real roots for $\alpha = 2$ since 2 is not a real root of $P_\infty$.

As described in section 3.1 and according to Theorem 1, one needs to perform the following two computations to prove the Theorem 5:

- for $i = 0\ldots3$, take any rational number $\beta_i \in ]\alpha_i, \alpha_{i+1}[$ and count the number of real roots of $\mathcal{S} \cup \{\alpha = \beta_i\}$ which is the constant number of real roots of all systems $\mathcal{S} \cup \{\alpha = \gamma_i\}$ with $\gamma_i \in ]\alpha_i, \alpha_{i+1}[$.

- for each $\alpha_i$, $i = 0 \dots 3$, solve the system $\mathcal{S} \cup \{\alpha = \alpha_i\}$.

In the first case, one needs to solve systems with a finite number of complex roots and to compute the sign of the polynomials from $\mathcal{F} = \{X_1, X_2, X_3, X_4\}$ at each root. In the second case, one may get systems with an infinite number of complex solutions (if $\alpha$ belongs to $O_\infty$). Such a case occurs only if $\alpha = 1$ or $\alpha = 3$. Since the $\alpha_i$ are real numbers, one will solve symbolically the systems $S_1 = \{\alpha = 1, g = 0, f > 0, g \in \mathcal{E}', f \in \mathcal{F}\}, S_2 = \{\alpha = 2, g = 0, f > 0, g \in \mathcal{E}', f \in \mathcal{F}\}, S_3 = \{\alpha = 3, g = 0, f > 0, g \in \mathcal{E}', f \in \mathcal{F}\}$ in order to avoid numerical approximations. Thus, for both problems, one has to compute the number of real roots of a system with rational coefficients and the sign of some polynomials at these roots. Let's describe now the main tools we used.

The first computation is to select $\beta_i$, which are rational numbers contained in the intervals $]\alpha_i, \alpha_{i+1}[$. We take $\beta_0 = 1/2, \beta_1 = 3/2, \beta_2 = 5/2, \beta_3 = 4$. After obtaining $\beta_i$, we solve $\{\alpha = \beta_i, g = 0, f > 0, g \in \mathcal{E}', f \in \mathcal{F}\}, i = 0..3$ and $\{\alpha = \alpha_i, g = 0, f > 0, g \in \mathcal{E}', f \in \mathcal{F}\}, i = 0 \dots 3$. Applying the algorithm described in section 3.2.3, we know that the system (14) always has

- 5 real roots for $\alpha \in ]0, 1[$, and
- 1 real root over the range $\alpha \in ]1, 2[$, $\alpha \in ]2, 3[$ and $]3, +\infty[$.

In order to get a complete result, one need finally to study the situations where $\alpha = 1$, $\alpha = 2$ and $\alpha = 3$.

The first case we need to study is $\alpha = 3$. We compute a lexicographic Gröbner basis with $X_1 > X_2 > X_3 > X_4$ which contains the polynomial $(12X_4^4 - 4X_4^2 + 1)(X_4 - X_3)(X_4 + X_3)$. Since $12X_4^4 - 4X_4^2 + 1$ has no real roots, all admissible solutions verify $X_4 - X_3 = 0$. We add this constraint into the systems. It shows that lexicographic Gröbner basis contains the polynomial $(X_2 - X_1)(X_2 + X_1)$. We add $X_2 - X_1$ and $X_4 - X_3$ into the system and its Gröbner basis then contains the polynomial $w(3w^2 - 1)$. Adding $X_2 - X_1$, $X_4 - X_3$ and $3X_4^2 - 1$ to the system, the lexicographic Gröbner basis is then $\{X_1 - X_2, 3X_2^2 - 1, X_4 - X_3, 3X_4^2 - 1\}$ and the only admissible solution for $\alpha = 3$ is thus $\beta = \{X_1 = X_2 = X_3 = X_4 = \frac{1}{\sqrt{3}}\}$.

By computing a Gröbner basis for $\alpha = 2$, one can check immediately that the system $\{\alpha = 2, g = 0, g \in \mathcal{E}'\}$ is zero-dimensional. Applying the algorithm described in section 3.2.3, one can find that it has only one solution with all positive coordinates, which is thus $\beta = \{X_1 = X_2 = X_3 = X_4 = \frac{1}{\sqrt{3}}\}$.

Let us now study the case $\alpha = 1$. By computing a Gröbner basis for a lexicographic ordering with $X_1 > X_2 > X_3 > X_4$, one of the polynomials in the basis is

$$(2\,X_4 + 1)\,(2\,X_4 - 1)\left(6\,{X_4}^2 + 6\,X_4 + 1\right)\left(6\,{X_4}^2 - 6\,X_4 + 1\right)\left(3\,{X_3}^2 - 2 + 3\,{X_4}^2\right) \qquad (26)$$

From (26) , one can easily find that only the following three cases $2X_4 - 1 = 0$, $6X_4^2 - 6X_4 + 1 = 0$, $3X_3^2 - 2 + 3X_3^2 = 0$ are need to consider since the other subsystems have clearly no admissible solutions. Moreover, one can check that both systems $\{\alpha = 1, 2X_4 - 1 = 0, g = 0, g \in \mathcal{E}'\}$ and $\{\alpha = 1, 6X_4^2 - 6X_4 + 1 = 0, g = 0, g \in \mathcal{E}'\}$ have a finite number of solutions. In order to simplify the study, we compute their roots with a unique system of equations $\{\alpha = 1, (2X_4 - 1)(6X_4^2 - 6X_4 + 1) = 0, g = 0, g \in \mathcal{E}'\}$ using the method described in section 3.2.3. Direct computation shows that there are 3 admissible solutions for $\alpha = 1$ and $(2X_4 - 1)(6X_4^2 - 6X_4 + 1) = 0$. For $\alpha = 1$ and $3X_3^2 - 2 + 3X_4^2 = 0$, we compute a lexicographic Gröbner basis with $X_1 > X_2 > X_3 > X_4$. It contains the polynomial $(X_2 - X_4)(X_2 + X_4)$ so that one can restrict the computations by adding $(X_2 - X_4)$ to the system. We again compute a lexicographic Gröbner basis with $X_1 > X_2 > X_3 > X_4$. It contains the polynomial $X_4(X_1 - X_3)$ so that one can again restrict the computations by adding $(x - z)$ to the system. Finally, adding $X_2 - X_4$ and $X_1 - X_3$ to the system, the lexicographic Gröbner basis is $\{X_1 - X_3, X_2 - X_4, 3X_3^2 - 2 + 3X_4^2\}$. The system has thus an infinite number of solutions $\{X_1 = X_3, X_2 = X_4, X_3 = \sqrt{\frac{2-3X_4^2}{3}}, |X_4| > \sqrt{\frac{2}{3}}\}$.

# 5 Convergence Analysis

Based on Theorem 5, we now investigate the selection criterion on $\alpha$ for global convergence. We start from the range of $\alpha \in ]1, \infty[$. From Theorem 5, we know that (14) has only one solution ($|g_{11}| = |g_{12}| = |g_{21}| = |g_{22}| = \frac{1}{\sqrt{3}}$ ) if $\alpha > 1$. Substituting this solution into (6), we can easily find

$$\begin{aligned} g_{11}^* g_{21} + g_{12}^* g_{22} &= 0 \\ g_{11}^* g_{12} + g_{21}^* g_{22} &= 0. \end{aligned} \tag{27}$$

In this case, the extended Hessian matrix (7) can be determined as follows

$$\mathbf{H}_G J = \begin{bmatrix} \mathbf{E}_G J & \mathbf{S}_G J \\ \mathbf{S}_G^* J & \mathbf{E}_G^* J \end{bmatrix} \tag{28}$$

where $\mathbf{E}_G J$ takes the following form

$$\mathbf{E}_G J = \begin{bmatrix} \frac{2+\alpha}{3} & (4-\alpha) g_{11}^* g_{12} & 0 & 0 \\ (4-\alpha) g_{11} g_{12}^* & \frac{2+\alpha}{3} & 0 & 0 \\ 0 & 0 & \frac{2+\alpha}{3} & (-4+\alpha) g_{11}^* g_{12} \\ 0 & 0 & (-4+\alpha) g_{11} g_{12}^* & \frac{2+\alpha}{3} \end{bmatrix}. \tag{29}$$

$\mathbf{S}_G J$ can be obtained by

$$\mathbf{S}_G J = \begin{bmatrix} 2(g_{11}^*)^2 & 4 g_{11}^* g_{12}^* & \alpha g_{11}^* g_{21}^* & \alpha g_{12}^* g_{21}^* \\ 4 g_{11}^* g_{12}^* & 2(g_{12}^*)^2 & \alpha g_{11}^* g_{22}^* & \alpha g_{12}^* g_{22}^* \\ \alpha g_{11}^* g_{21}^* & \alpha g_{11}^* g_{22}^* & 2(g_{21}^*)^2 & 4 g_{21}^* g_{22}^* \\ \alpha g_{12}^* g_{21}^* & \alpha g_{12}^* g_{22}^* & 4 g_{21}^* g_{22}^* & 2(g_{22}^*)^2 \end{bmatrix}. \tag{30}$$

Hence, the determinants of the first five upper left submatrices of $\mathbf{H}_G J$ are

$$\begin{cases} \Delta_1 = \frac{2+\alpha}{3} \\ \Delta_2 = \frac{4(\alpha-1)}{3} \\ \Delta_3 = \frac{4(\alpha-1)(2+\alpha)}{9} \\ \Delta_4 = \frac{16(\alpha-1)^2}{9} \\ \Delta_5 = \frac{32\alpha(1-\alpha)}{27}. \end{cases} \tag{31}$$

It is apparent that $\Delta_5$ will always be negative if $\alpha$ is selected from the range of $]1,\infty[$. Hence, $\mathbf{H}_G J$ will not be (semi)positive definite in this case and the CC-CMA will be a globally convergent algorithm is the mixing parameter is larger than 1.

Now, let us consider the case that $\alpha = 1$. It is easy to see that $g_{11} = \frac{\sqrt{2}}{10}$ , $g_{12} = \frac{\sqrt{582}}{30}$, $g_{21} = -g_{11}$ and $g_{22} = g_{12}$ are one of the solutions of the equations in (6) and satisfy $g_{11}g_{12}^* g_{21}^* g_{22} = g_{11}^* g_{12} g_{21} g_{22}^* = -\frac{97}{7500}$. For this undesired stationary point, the eigenvalues of the Hessian matrix $\mathbf{H}_G J$ can be obtained as follows

$$\lambda_1 = 4, \quad \lambda_2 = \frac{4}{3} + \frac{4\sqrt{291}}{75}, \quad \lambda_3 = 4/3,$$
$$\lambda_4 = \frac{4}{3} - \frac{4\sqrt{291}}{75}, \quad \lambda_n = 0 \ \text{ for } n = 5, \cdots, 8. \tag{32}$$

Since these eigenvalues are nonnegative, $\mathbf{H}_G J$ is positive semidefinite. In other words, this undesirable stationary point will be a candidate for a local minima of the CC-CMA. To check whether this point is a local minima or not, we consider the following perturbation

$$g_{ij}^+ = g_{ij} + \varepsilon_x + \varepsilon_y \jmath, \quad i,j = 1..2 \tag{33}$$

where $\varepsilon_x$ are $\varepsilon_x$ very small positive numbers, $\jmath = \sqrt{-1}$. Substituting these $g_{ij}^+$ into (5), we can easily obtain

$$\begin{aligned} J^+ - J &= \frac{782}{75}\varepsilon_x^2 + \frac{194}{75}\varepsilon_y^2 + \frac{16\sqrt{582}}{15}\varepsilon_x^3 + \frac{16\sqrt{582}}{15}\varepsilon_x\varepsilon_y^2 + 32\varepsilon_x^2\varepsilon_y^2 + 16\varepsilon_x^4 + 16\varepsilon_y^4 \\ &\approx \frac{782}{75}\varepsilon_x^2 + \frac{194}{75}\varepsilon_y^2 > 0. \end{aligned} \tag{34}$$

Clearly, this undesired stationary point is a local minimum and the CC-CMA will not converge globally when $\alpha = 1$.

Then, we study the case that $\alpha \in ]0,1[$. From theorem 5 we know that the real solutions of (14) form 5 non intersecting continuous branches over $]0,1[$, including $(\alpha,\beta)_{\alpha\in]0,1[}$. We now show that $\Delta_2$ or $\Delta_4$ is negative over each of these branches so that $\mathbf{H}_G J$ is never (semi)positive when $\alpha \in ]0,1[$. Since these branches are non intersecting and continuous, one first shows that $\Delta_4$ has constant sign by proving that it never vanishes : by computing a Gröbner basis of $\{\Delta_4, \mathcal{E}'\}$, where $\mathcal{E}'$ is the set of polynomials defining the equations of (14) for a block ordering eliminating all the variables but $\alpha$ (see section 3.2.2), one gets a univariate polynomial $p(\alpha)$ with no real roots in $]0,1[$. Since the roots of this polynomial are the projections on the $\alpha$-axis of the zeroes of the ideal $\langle \Delta_4, \mathcal{E}' \rangle$ (Proposition 1), $\Delta_4$ never vanishes on the solution branches over $]0,1[$. Since the branches are continuous, $\Delta_4$ as constant sign on each of these branches.

We now show that $\Delta_4$ is positive on $(\alpha,\beta)_{\alpha\in]0,1[}$ and negative on all the other branches over $]0,1[$. We choose an arbitrary value $\alpha_0 \in ]0,1[$, solve the zero-dimensional system obtained by replacing $\alpha$ by $\alpha_0$ in (14) and use the extended RUR to get the sign of $\Delta_4$ at each of the five real solutions using the algorithm (extended RUR) from section 3.2.3. We find that $\Delta_4$ is negative at 4 roots and positive at one root. Since the branches are non intersecting and continuous over $]0,1[$, and since $\Delta_4$ never vanishes on a branch, one deduce that $\Delta_4$ is negative on 4 branches and positive on 1 branch and it is easy to check that it is positive on the branch $(\alpha,\beta)_{\alpha\in]0,1[}$.

It is easy to check that $\Delta_4$ is negative on the branch $(\alpha,\beta)_{\alpha\in]0,1[}$ which proves that $\Delta_2$ or $\Delta_4$ is negative on each branch over $]0,1[$ and thus that $\mathbf{H}_G J$ is never (semi)positive when $\alpha \in ]0,1[$.

# 6 Numerical Results

In this section, we first give the numerical examples to examine the root distribution of system (14) for $0 < \alpha < 1$. From Tab. 1, we can easily find that (14) always has five solutions when $\alpha = 0.9$, $\alpha = 0.5$ and $\alpha = 0.3$. Notice that the solution 5 in Tab. 1 corresponds to $\beta$ in Theorem 5. Clearly, these examples confirm the theoretical analysis of Theorem 5. The determinants of the first four upper left submatrices of $\mathbf{H}_G J$ at these solutions, as presented in Tab. 2, support the convergence analysis of the CC-CMA for the case $0 < \alpha < 1$. From Tab. 2, we can see that $\Delta_1$ always takes positive values and $\Delta_4$ is shown to be negative except for the solution $\beta$. As for $\Delta_2$ and $\Delta_3$, there always exist 3 solutions for system (14) including $\beta$ which make them negative. Hence, if $0 < \alpha < 1$, each solution for system (14) will make at least one of principal minors of Hessian matrix negative.

Then, we consider a communication system with two users transmitting MPSK signals. These source signals are received by three receivers. On the receiver side, additive white Gaussian noise of SNR=20 dB is added to each of the three received signals. The following weight update function is used in all simulations

$$\mathbf{w}_i(n+1) = \mathbf{w}_i(n) - \mu \nabla_{\mathbf{w}_i} J(n) \tag{35}$$

where $\mu$ is the step size and $\nabla_{\mathbf{w}_i} J(n)$ is the gradient vector of $J$ w.r.t $\mathbf{w}_i$, which can be expressed as follows

$$\nabla_{\mathbf{w}_i} J(n) = 2E[(|y_i|^2 - 1)y_i^* \mathbf{x}] + \alpha \sum_{j=1, j\neq i}^{K} E[y_i^* y_j] E[y_j^* \mathbf{x}]. \tag{36}$$

In our simulations, the step size $\mu$ takes 0.0001.

The first simulation is to illustrate the existence of undesired stationary points when $\alpha = 1$. We consider a simple case of $3 \times 2$ matrix channel chosen as

$$\mathbf{A} = \begin{bmatrix} 0.6831 + 0.0164\jmath & 0.6124 + 0.0576\jmath \\ 0.0928 + 0.1901\jmath & 0.6085 + 0.3676\jmath \\ 0.0353 + 0.5689\jmath & 0.0158 + 0.6315\jmath \end{bmatrix}.$$

The CC-CMA was run with the following initial separating matrix

$$\mathbf{W} = \begin{bmatrix} 0.7176 + 0.4544\jmath & 0.6927 + 0.4418\jmath & 0.0841 + 0.3533\jmath \\ 0.1536 + 0.7275\jmath & 0.6756 + 0.4784\jmath & 0.6992 + 0.5548\jmath \end{bmatrix}.$$

The CC-CMA reaches the following setting after it converges

$$\mathbf{G} = \begin{bmatrix} -0.9116 - 0.1071\jmath & -0.1292 + 0.0865\jmath \\ -0.7173 - 0.5448\jmath & -0.0160 - 0.1787\jmath \end{bmatrix}.$$

Clearly, the separation of sources was not achieved by the CC-CMA in this case.

The second simulation is to investigate the convergence performance of CC-CMA if $\alpha \neq 1$. In this simulation, the performance is first evaluated by the interference-signal ratio (ISR) of $i$th source at the $k$th output, which is defined as follows

$$ISR_i[\mathbf{w}_k] \ \ (dB) = 10 \times log_{10}\left(\frac{|g_{ki}|^2}{\sum_{l=1,l\neq i}^{K} |g_{kl}|^2}\right) \tag{37}$$

where $g_{kl} = \mathbf{w}_k^H \mathbf{a}_l$, $\mathbf{a}_l$ is the $l$th col in matrix $\mathbf{A}$. The ISR index is estimated by averaging 50 runs with 5000 symbols. In each independent experiment, the channel and initial separating matrix are randomly chosen from a complex Gaussian matrix with distribution of zero mean and unit variance. From Fig.1, we can easily find that the ISR can be significantly suppressed by the CC-CMA if $\alpha \neq 1$, which confirms the expecting convergent behavior.

# 7 Conclusion

We have introduced a new method for global convergence analysis of the CC-CMA. By solving semi-algebraic sets, we proved, when the CC-CMA is utilized to separate the MPSK sources, it can converge globally if the mixing parameter is not selected as 1. The most appealing feature of our approach is that it provides a general frame for convergence analysis of a family of stochastic gradient algorithm since the proposed approach does not exploit the structural properties of the CC-CMA. Hence, it can be extended to convergence analysis of other stochastic gradient algorithms. Another advantage of our approach is the computation efficiency. Based on diriment variety, we proposed an optimal algorithm to solve semi-algebraic sets, which only yields the necessary information for the studied problem.

# References

[1] J. Bochnak M. Coste, and M. F. Roy, "Géométrie algébrique réelle", *Ergebnisse der Mathematik* , Berlin: Springer-Verlag, 1987.

[2] S. Basu, R. Pollack, and M. F. Roy, "Algorithms in real algebraic geometry", *Algorithms and Computations in Mathematics*, New York:Springer-Verlag, 2003.

[3] B. Buchberger, "Gröbner bases : an algorithmic method in polynomial ideal theory", in "Recent trends in multidimensional systems theory", editored by N. K. Bose, Reidel Publishing Company, 1985.

[4] T. Becker and V. Weispfenning,"Groebner bases: a computational approach to commutative algebra", *Graduate Texts in Mathematics: readings in mathematics*, New York:Springer-Verlag, 1993.

[5] A. M. Bronstein, M. M. Bronstein, M. Zibulevsky, "Relative optimization for blind deconvolution Bronstein", *IEEE Trans. Signal Processing*, vol. 53, no. 6, pp. 2018-2026, June. 2005.

[6] L. Castedo, C. J. Escudero, and A. Dapena, " A Blind Signal Separation Method for Multiuser Communications ", *IEEE Trans. Signal Processing*, vol. 45, no. 5, pp. 1343-1348, May. 1997.

[7] G. E. Collins, "Quantifier elimination for real closed fields by cylindrical algebraic decomposition", *Springer Lecture Notes in Computer Science* ,vol. 33, pp. 515-532, 1975.

[8] G. E. Collins and H. Hong, "Partial cylindrical algebraic decomposition", *Journal of Symbolic Computation*, vol. 12, no. 3, pp. 299-328, June. 1991.

[9] D. Cox, J. Little and D. O'Shea, "Ideals, varieties, and algorithms an introduction to computational algebraic geometry and commutative algebra", New York: Springer-Verlag, 1992.

[10] A. Dapena and L. Castedo, "Stochastic gradient adaptive algorithms for blind source separation", *Signal Processing*, vol. 75, no. 1, pp. 11-27, Jan. 1999.

[11] C. J. Escudero, L. Castedo, U. Mitra, "A modified CMA equalizer for the removal of length dependent local minima in AR channels", *IEEE Trans. Signal Processing*, vol. 47, no. 2, pp. 540-544, Feb. 1999.

[12] J. C. Faugère, "A New Efficient Algorithm for Computing Gröbner bases ($F_4$)", *Journal of Pure and Applied Algebra*, vol. 139, no. 1-3, pp. 61-88, 1999.

[13] D. Z. Feng, X. D. Zhang, D. X. Chang, and W. X. Zheng, "A fast recursive total least squares algorithm for adaptive FIR filtering" , *IEEE Trans. Signal Processing* , vol. 52, no. 10, pp. 2729-2737, Oct. 2004.

[14] D. N. Godard, "Self-recovering equalization and carrier tracking in two-dimensional data communication systems", *IEEE Trans. Commun.*, vol. 28, no. 11, pp. 1867-1875, Nov. 1980.

[15] S. Haykin, "Adaptive Filter Theory" (4th ed.), New York: Prentice Hall, 2001.

[16] S. Lambotharan and J. Chambers, "On the surface characteristics of a mixed constant modulus and cross-correlation criterion for the blind equalization of a MIMO channel", *Signal Processing*, vol. 74, no. 2, pp. 209-216, Apr. 1999.

[17] D. Lazard and F. Rouillier, "Solving Parametric Polynomial Systems", accepted by *Jounal of Symb. Compu.* with minor revision.

[18] Y. Luo, J. Chambers, and S. Lambotharan, "Global convergence and mixing parameter selection in the cross-correlation constant modulus algorithm for the multi-user environment", *IEE Proc.-Vis. Image Signul Process*, vol. 148, no. 1. pp. 9-20, Feb. 2001.

[19] R. K. Martin, J. Balakrishnan, W. A. Sethares, and C. R. Johnson, "A blind adaptive TEQ for multicarrier systems ", *IEEE Signal Processing Lett.*, vol. 9, no. 11, pp.341-343, Nov. 2002.

[20] D. Mumford, "Algebraic Geometry I, Complex Projective Varieties", New York: Springer-Verlag, 1976.

[21] C. B. Papadias and A. Paulraj, "A space-time constant modulus algorithm for SDMA systems", Proc. IEEE/VTS 46th Veh. Technol. Conf. (VTC-96), pp. 86-90, Atlanta, GA, Apr. 1996.

[22] C. B. Papdiaus and C. Paulraj, "A constant modulus algorithm for multi-user signal separation in presence of delay spread using antenna arrays", *IEEE Signal Process. Lett.*, vol. 4, no. 6, pp. 178-181, Jun. 1997.

[23] C. B. Papadias, "Globally convergent blind source separation based on a multiuser kurtosis maximization criterion", *IEEE Trans. Signal Processing*, vol. 48, no. 12, pp. 3508-3519, Dec. 2000.

[24] J. M. Paez Borrallo, F. L. Speranzini, "Convergence analysis of decision-directed adaptive echo cancellers for baseband data transmission", *IEEE Trans. on Commun.*, vol. 43, no. 234, pp. 503-513, Feb. 1995.

[25] A. J. Paulraj and C. B. Papadias, "Space-time processing for wireless communications", *IEEE Signal Processing Mag.*, vol. 14, no. 6, pp. 49-83, Nov. 1999.

[26] F. Rouillier, "Solving zero-dimensional systems through the rational univariate representation", *Journal of Appl. Algebr. Eng. Comm.*, vol. 9 no. 5, pp. 433-461, May. 1999.

[27] N. Revol and F. Rouillier, "Motivations for an arbitrary precision interval arithmetic and the MPFI library", *Reliable Computing*, vol. 11, pp. 1-16, 2005.

[28] F. Rouillier and P. Zimmermann, "Efficient Isolation of Polynomial Real Roots", *J. Comput. Appl. Math*, vol. 162, no. 1, pp. 33-50, 2003.

[29] R. Schober, W. H. Gerstacker, and J. B. Huber, "Adaptive noncoherent linear minimum ISI equalization for MDPSK and MDAPSK signals", *IEEE Trans. Signal Processing*, vol. 49, no. 9, pp. 2018-2030, Sept. 2001.

[30] A. Touzni,I. Fijalkow, M. G. Larimore, and J. R. Treichler, "A globally convergent approach for blind MIMO adaptive deconvolution", *IEEE Trans. Signal Processing*, vol. 49, no. 6, pp. 1166-1178, Jun. 2001.

[31] J. R. Treichler and B. G. Agee, "A new approach to multipath correction of constant modulus signals", *IEEE Trans. Signal Processing*, vol.31, no.2, pp. 459-472, Feb. 1983.

[32] V. Weispfenning, "Comprehensive Gröbner base", *J. Symb. Comput.*, vol. 14, no. 1, pp. 1-29, Jan. 1992.

[33] V. Weispfenning, "Cannoical Comprehensive Gröbner bases", Proc. 2002 International symposium on symbolic and algebraic compuation, pp. 270-276, 2002.

[34] C. Xu, G. Feng, and K. S. Kwak, "A modified constrained constant modulus approach to blind adaptive multiuser detection", *IEEE Trans. Commun*, vol. 49, no. 9, pp. 1642-1648, Sept. 2001.

Tab 1. Root Distribution of System (14)

| | Solution 1 | Solution 2 | Solution 3 | Solution 4 | Solution 5 | |
|---|---|---|---|---|---|---|
| $\lvert g_{11}\rvert$ | 0.2883959547 | 0.7263007579 | 0.8558321519 | 0.1534046182 | 0.5773502692 | $\alpha$ |
| $\lvert g_{12}\rvert$ | 0.7263007579 | 0.2883959547 | 0.1534046182 | 0.8558321519 | 0.5773502692 | $=$ |
| $\lvert g_{21}\rvert$ | 0.1534046182 | 0.8558321519 | 0.7263007579 | 0.2883959547 | 0.5773502692 | 0.9 |
| $\lvert g_{22}\rvert$ | 0.8558321519 | 0.1534046182 | 0.2883959547 | 0.7263007579 | 0.5773502692 | |
| $\lvert g_{11}\rvert$ | 0.6488184703 | 0.4297639180 | 0.0792841748 | 0.9423648905 | 0.5773502692 | $\alpha$ |
| $\lvert g_{12}\rvert$ | 0.4297639180 | 0.6488184703 | 0.9423648905 | 0.0792841748 | 0.5773502692 | $=$ |
| $\lvert g_{21}\rvert$ | 0.9423648905 | 0.0792841748 | 0.4297639180 | 0.6488184703 | 0.5773502692 | 0.5 |
| $\lvert g_{22}\rvert$ | 0.0792841748 | 0.9423648905 | 0.6488184703 | 0.4297639180 | 0.5773502692 | |
| $\lvert g_{11}\rvert$ | 0.6198037839 | 0.4980680376 | 0.0481030782 | 0.9695407645 | 0.5773502692 | $\alpha$ |
| $\lvert g_{12}\rvert$ | 0.4900884980 | 0.6198037839 | 0.9695407645 | 0.0481030782 | 0.5773502692 | $=$ |
| $\lvert g_{21}\rvert$ | 0.9695407645 | 0.0481030782 | 0.4900884980 | 0.6198037839 | 0.5773502692 | 0.3 |
| $\lvert g_{22}\rvert$ | 0.0481030782 | 0.9695407645 | 0.6198037839 | 0.4900884980 | 0.5773502692 | |

Tab 2. Principals of Hessian matrix (7) at the solutions of (14)

| | Solution 1 | Solution 2 | Solution 3 | Solution 4 | Solution 5 | |
|---|---|---|---|---|---|---|
| $\Delta_1$ | 0.46391974970 | 1.10194387600 | 1.498688108 | 1.09878160100 | 0.9666666667 | $\alpha$ |
| $\Delta_2$ | -0.0067388132 | -0.0067388132 | 1.533405480 | 0.37324157820 | -0.133333333 | $=$ |
| $\Delta_3$ | -0.3049293306 | -0.1353577117 | 1.393055746 | 0.05482432938 | -0.1288888886 | 0.9 |
| $\Delta_4$ | -0.8538287786 | -0.4153607486 | -1.02525789 | -0.2622629445 | 0.2311111107 | |
| $\Delta_1$ | 0.8666755242 | 0.4257927209 | 1.669698781 | 1.787832973 | 0.8333333334 | $\alpha$ |
| $\Delta_2$ | -0.7930550411 | -0.7930550412 | 2.959721706 | 2.959721706 | -0.6666666662 | $=$ |
| $\Delta_3$ | -1.453332679 | -1.396385996 | 1.111241877 | 2.425976796 | -0.5555555552 | 0.5 |
| $\Delta_4$ | -2.415443657 | -4.604926883 | -5.230389673 | -3.040906446 | 1.037037037 | |
| $\Delta_1$ | 0.7793766539 | 0.4980680376 | 1.841348821 | 1.884539820 | 0.7666666667 | $\alpha$ |
| $\Delta_2$ | -1.054322777 | -1.054322777 | 3.460989443 | 3.460989443 | -0.933333333 | $=$ |
| $\Delta_3$ | -2.001855297 | -1.964757303 | 1.667272025 | 2.642173906 | -0.715555555 | 0.3 |
| $\Delta_4$ | -3.666556336 | -6.669475768 | -6.97651700 | -3.97359757 | 1.368888889 | |

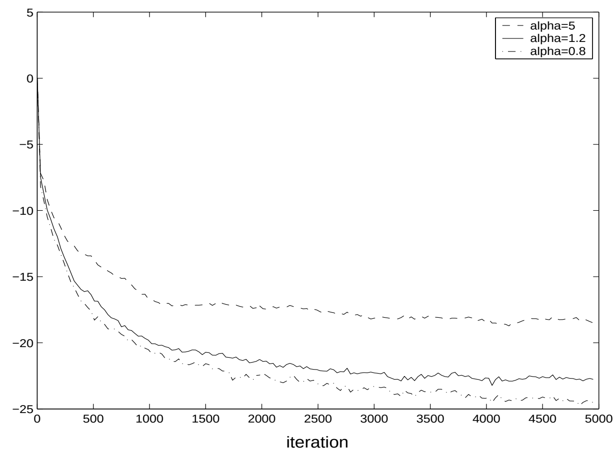


Figure 1(a). ISR for User 1

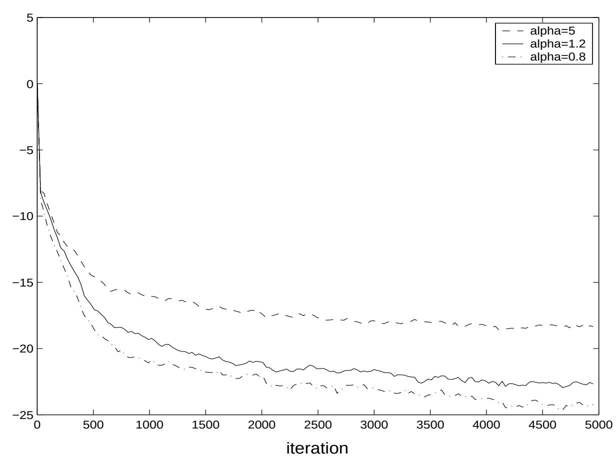


Figure 1(b). ISR for User 2

# Contents

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399